United States General Accounting Office

GAO

Report to the Ranking Minority Member, Committee on Energy and Commerce, House of Representatives

April 2002

FINANCIAL PRIVACY

Status of State Actions on Gramm-Leach-Bliley Act's Privacy Provisions

GAO-02-361

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
00MAY2002	N/A	-

Title and Subtitle FINANCIAL PRIVACY: Status of State Actions on Gramm-Leach- Bliley Acts Privacy Provisions	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) U.S. General Accounting Office 441 G Street NW, Room LM Washington, D.C. 20548	**Performing Organization Report Number** GAO-02-361
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	

Abstract
This report responds to your request for information on what states have done to implement the information privacy provisions of the Gramm- Leach-Bliley Act (GLBA) of 1999 as they pertain to insurance providers.1 In Subtitle A of Title V of GLBA, Congress established the policy that each financial institution, which is defined to include most insurance providers or companies, has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers nonpublic personal information. 2 The subtitle applies this policy by generally prohibiting financial institutions from disclosing consumers nonpublic personal information to any entity that is not an affiliate3 of or related by common ownership or control to the institution (nonaffiliated third party), unless the consumer is given an opportunity to opt out of such disclosure. Also, financial institutions must provide consumers with privacy notices that, among other things, explain an institutions policies and practices for disclosing and protecting the privacy of nonpublic personal information. Subtitle A calls upon federal regulators to (1) issue regulations implementing these disclosure-related requirements and (2) establish standards for safeguarding the privacy and15 U.S.C. § 6801(a). Subtitle A defines nonpublic personal information as personally identifiable financial information that an institution obtains under any of the following three sets of circumstances: (1) the consumer provides the information to the institution to obtain a financial product or service; (2) the information is about the consumer and results from any transaction involving a financial product or service between the institution and the consumer; or (3) the information is about the consumer and is otherwise obtained in connection with providing a financial product or service to that consumer. Nonpublic personal information also includes lists or groupings of consumers derived from nonpublic personally identifiable information.

Subject Terms

Report Classification	**Classification of this page**
unclassified	unclassified
Classification of Abstract	**Limitation of Abstract**
unclassified	SAR

Number of Pages
22

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

April 12, 2002

The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

Dear Mr. Dingell:

This report responds to your request for information on what states have done to implement the information privacy provisions of the Gramm-Leach-Bliley Act (GLBA) of 1999 as they pertain to insurance providers.[1] In Subtitle A of Title V of GLBA, Congress established the policy that each financial institution, which is defined to include most insurance providers or companies, has "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." [2] The subtitle applies this policy by generally prohibiting financial institutions from disclosing consumers' nonpublic personal information to any entity that is not an affiliate[3] of or related by common ownership or control to the institution (nonaffiliated third party), unless the consumer is given an opportunity to opt out of such disclosure. Also, financial institutions must provide consumers with privacy notices that, among other things, explain an institution's policies and practices for disclosing and protecting the privacy of nonpublic personal information. Subtitle A calls upon federal regulators to (1) issue regulations implementing these disclosure-related requirements and (2) establish standards for safeguarding the privacy and

[1]These provisions are set forth in Subtitle A of Title V of GLBA, Pub. L. No. 106-102 §§ 501 – 510, 15 U.S.C. §§ 6801-6809 (2000).

[2]15 U.S.C. § 6801(a). Subtitle A defines nonpublic personal information as personally identifiable financial information that an institution obtains under any of the following three sets of circumstances: (1) the consumer provides the information to the institution to obtain a financial product or service; (2) the information is about the consumer and results from any transaction involving a financial product or service between the institution and the consumer; or (3) the information is about the consumer and is otherwise obtained in connection with providing a financial product or service to that consumer. Nonpublic personal information also includes lists or groupings of consumers derived from nonpublic personally identifiable information.

[3]Under Subtitle A, the term "affiliate" means any company that controls, is controlled by, or is under common control with another company.

integrity of customer information and records.[4] Concerning insurance providers, which are state-regulated, Subtitle A calls upon state insurance authorities to enforce its provisions and to adopt implementing regulations regarding both information disclosure and information safeguards.

To facilitate a uniform state approach to implementing the disclosure-related provisions of Subtitle A, the National Association of Insurance Commissioners (NAIC) issued its "Privacy of Consumer Financial and Health Information Regulation" (2000 Model Regulation) on September 26, 2000. In most respects, the 2000 Model Regulation reflects the comparable disclosure-related regulations promulgated by federal depository institution regulators and the Federal Trade Commission (FTC).[5] The 2000 Model Regulation follows an earlier effort by NAIC to protect the privacy and accuracy of personal information obtained by insurance industry participants in connection with insurance transactions. Specifically, in 1982 NAIC issued the Insurance Information and Privacy Protection Model Act (1982 Model Act).

In your letter, you expressed concerns regarding the progress that states are making in promulgating regulations under Subtitle A. Our objectives in this review were to (1) report on the actions taken by the states to carry out the disclosure-related provisions of Subtitle A relating to the insurance industry and (2) ascertain the progress that states have made in implementing the Subtitle A mandate that they establish standards for safeguarding insurance customer records and information.

To ascertain the specific legislative and regulatory actions taken by the states to carry out the provisions of Subtitle A relating to the insurance industry, we primarily used publicly available data from NAIC. We also sent a questionnaire to those state insurance authorities that continue to rely on insurance privacy laws based on the 1982 Model Act. To ascertain the progress that states have made in implementing the Subtitle A mandate that they establish standards for safeguarding insurance customer records

[4]The federal regulators responsible for issuing Subtitle A regulations are the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Federal Trade Commission, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, secretary of the Department of the Treasury, Commodity Futures Trading Commission, and Securities and Exchange Commission.

[5]For this report, federal depository institution regulators are the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

and information, we reviewed the NAIC model draft for safeguarding standards and collected information from the NAIC Privacy Working Group, which was tasked with developing the draft standards.

Results in Brief

As of March 1, 2002, all of the states and the District of Columbia have taken some action to ensure that insurance companies under their jurisdiction meet Subtitle A's disclosure and notice requirements. In addition, some states have included or retained provisions in their regulations or laws that, in their respective views, provide greater protections or more restrictive requirements than those contained in Subtitle A. Thirty-five states and the District of Columbia have adopted NAIC's 2000 Model Regulation, although 2 of those states—Vermont and New Mexico—substituted an affirmative consent requirement (opt in) for the 2000 Model Regulation's opt-out provision. One state, Alaska, was in the process of finalizing regulations to implement the requirements of Subtitle A. The remaining 14 states had previously enacted laws that were based on NAIC's 1982 Model Act and have either amended these laws or taken some administrative measures to ensure compliance with all of Subtitle A's provisions.

Only one state, New York, has established standards for protecting the security and confidentiality of insurance customer information as of March 1, 2002. Another state, California, has issued proposed regulations establishing such standards. In contrast, as of March 1, 2002, the federal regulators charged with implementing Subtitle A—with the exception of FTC—have issued their final standards. FTC has received comments on proposed standards and is developing its final rule. In early April, NAIC adopted a model regulation to assist the states in establishing the required standards. NAIC staff explained that the state insurance authorities were slower in establishing the standards due to a number of factors, such as the need to develop a flexible regulation to cover a wide range in the types and sizes of organizations. State insurance authorities still need to adopt the model standards, either by legislative or regulatory action or both. During this time period, insurance customers in these states may have reduced assurances that they have a level of legal protection over the security and confidentiality of their information that is consistent with that of the customers of banking and securities companies.

Background

In Subtitle A, Congress established a two-pronged approach for protecting the privacy of nonpublic personal information obtained by financial institutions. The subtitle establishes restrictions and requirements relating

to a financial institution's disclosure of nonpublic personal information to nonaffiliated third parties and calls upon federal regulators to promulgate and enforce regulations implementing those provisions. In addition, the federal regulators are to establish standards for safeguarding the security and confidentiality of financial institution customer records and information. The Subtitle A scheme contemplates that state insurance authorities will establish and enforce disclosure-related requirements as well as safeguarding standards.[6]

Under Subtitle A, a financial institution generally is prohibited from disclosing a consumer's protected information to nonaffiliated third parties unless the institution provides the consumer with a privacy notice and an opportunity to opt out of such disclosures.[7] A privacy notice must describe the institution's policies and practices for disclosing nonpublic personal information to nonaffiliated third parties. In addition, the privacy notice must include specific information about the categories of persons to whom information may be disclosed, a statement of the institution's policies and practices with respect to disclosing the protected information of persons who have ceased to be customers, the categories of protected information collected and disclosed by the institution, and the institution's policies for safeguarding the information. A financial institution generally may not disclose a consumer's nonpublic personal information to a nonaffiliated third party unless the institution provides a privacy notice (initial notice) to the consumer. In addition, for consumers who become customers of a financial institution, the institution must furnish the privacy notice when the customer relationship is established (initial customer notice) and annually (annual notice).[8]

[6]Subtitle A provides that if a state insurance authority fails to adopt regulations to carry out the subtitle, the state forfeits its eligibility under GLBA to override certain customer protection regulations promulgated by the federal depository institution regulators applicable to insurance sales by or at depository institutions. 15 U.S.C. § 6805(c) (2000).

[7]In addition, Subtitle A contains other disclosure restrictions. The subtitle generally prohibits disclosure of an account number or similar form of access number or access code for a credit card, deposit account, or transaction account to third parties for marketing purposes. Also, a nonaffiliated third party who receives protected information subject to the opt-out requirement may not disclose the information to anyone other than an affiliate of either the recipient or the financial institution that disclosed the information, unless the disclosure would be lawful if made directly by the disclosing institution.

[8]Under Subtitle A, a consumer is an individual (and his or her legal representative) who obtains from a financial institution a financial product or service that is to be used primarily for personal, family, or household purposes. A customer is a consumer who has established a customer relationship with the institution.

The opt-out notice must explain that nonpublic personal information may be disclosed to nonaffiliated third parties and that the consumer may opt out of the disclosure. The opt-out notice must, among other things, identify the categories of information that may be disclosed and the categories of nonaffiliated third parties to whom disclosures may be made. It also must inform the consumer of how to exercise the nondisclosure option. A consumer's failure to opt out within a reasonable time after having the opportunity to do so means that the financial institution may disclose the consumer's nonpublic information to nonaffiliated third parties.

The privacy notice and opt-out requirements are subject to certain exceptions. One exception, known as the joint marketing exception, releases a financial institution from the opt-out requirement when it discloses protected information to nonaffiliated third parties who are service providers or joint marketers. The exception specifically permits disclosures for the purpose of marketing the financial institution's products or services as well as financial products or services offered pursuant to a joint marketing agreement between the disclosing institution and other financial institutions, subject to restrictions on further disclosure of the information.

Subtitle A also contains two sets of exceptions from both the requirement to furnish an initial privacy notice to consumers (i.e., individuals who have interacted with the institution but who have not established a customer relationship) and the opt-out requirement. One set of exceptions permits the disclosure of nonpublic personal information without such notices as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, such as credit or insurance, and to maintain or service customer accounts. The other set of exceptions includes disclosures authorized by the consumer, disclosures to the consumer's authorized representative, disclosures in connection with protecting the confidentiality of institution records concerning the consumer, disclosures required for institutional risk control and other institutional purposes, and disclosures specifically permitted by laws or to comply with legal requirements.

All of the States Have Taken Action to Implement Subtitle A's Disclosure-Related Provisions

All of the states and the District of Columbia have by statute, regulation, or insurance bulletin advised the insurance institutions they regulate that the institutions must comply with Subtitle A's disclosure-related provisions. Of the 51 jurisdictions, all but Alaska have in place laws or regulations that are based on either the 2000 Model Regulation or the 1982 Model Act.[9] Thirty-five states and the District of Columbia are applying standards and requirements that are based on the 2000 Model Regulation developed by NAIC to help states achieve compliance with Subtitle A, although 2 jurisdictions—Vermont and New Mexico—changed a key provision of the 2000 Model Regulation to achieve greater privacy protection. The remaining 14 states (Model Act states) have relied upon their versions of the 1982 Model Act either as amended to reflect specific Subtitle A requirements not contained in the 1982 Model Act or in combination with administrative measures applying those requirements to insurance providers.[10] Four of the 14 Model Act states relaxed restrictions on disclosures for marketing purposes that are contained in the 1982 Model Act but are not imposed by Subtitle A or the 2000 Model Regulation.

NAIC's 2000 Model Regulation Generally Reflects Comparable Regulations of the Depository Institution Regulators

In most aspects, the 2000 Model Regulation, which was issued by NAIC to facilitate a uniform state approach to implementing the disclosure-related requirements of Subtitle A, closely tracks similar regulations issued by the federal depository institution regulators and FTC. The 2000 Model Regulation contains similar notice requirements, disclosure restrictions, and exceptions. However, the 2000 Model Regulation differs in two ways from Subtitle A and the regulations of the federal depository institution regulators and FTC.

One difference between Subtitle A and the 2000 Model Regulation pertains to the scope of individuals who qualify as consumers entitled to receive privacy and opt-out notices. For purposes of both Subtitle A and the 2000 Model Regulation, a consumer is defined as an individual (or the individual's legal representative) who seeks to obtain, obtains, or has

[9]Alaska enacted a statute requiring the director of the Division of Insurance to adopt privacy regulations "at least as restrictive" as the 2000 Model Regulation. Alaska issued a draft regulation for public comment that "sets standards that an insurance company and its representatives must comply with in order to disclose personal information about a consumer." The final regulation was still pending as of March 1, 2002.

[10]The 14 Model Act states are Arizona, California, Connecticut, Georgia, Maine, Massachusetts, Minnesota, Montana, Nevada, New Jersey, North Carolina, Ohio, Oregon, and Virginia.

obtained an insurance product or service from a licensee[11] that is to be used primarily for personal, family, or household purposes and about whom the licensee has nonpublic information. The 2000 Model Regulation is broader than the regulations of the federal depository institution regulators and FTC in that it specifies that beneficiaries of life insurance policies, claimants on policies, insured individuals, and mortgagors can qualify as consumers if an insurance provider discloses nonpublic personal information about such individuals and the disclosure is not subject to an exception from opt-out and initial notice requirements. Moreover, the examples in the 2000 Model Regulation effectively broaden the definition of a consumer by including participants in and beneficiaries of employee benefits or workers' compensation plans as well as persons covered by group or blanket policies. Such individuals are considered to be consumers unless the licensee (1) provides initial, annual, and, if necessary, revised notices to the group or blanket policyholder and (2) does not disclose nonpublic personal financial information about the individuals unless permitted under generally the same exceptions provided under Subtitle A. In contrast, under the regulations of the federal depository institution regulators and FTC, these individuals are not consumers protected by Subtitle A because it is the plan sponsor or manager who obtained a financial product or service from the financial institution rather than the individuals covered by the plan.

The second difference between the 2000 Model Regulation and Subtitle A and the federal regulations relates to health information. The 2000 Model Regulation treats health information differently from other nonpublic personal information. It defines health information as information recorded in any form or medium that is created or derived from a health care provider or the consumer and relates to the consumer's health, the provision of health care to the consumer, or payment for health care services. Under the 2000 Model Regulation, an insurance provider is prohibited from disclosing health information to any person unless the consumer affirmatively authorizes the disclosure (opt in). This section of the 2000 Model Regulation is subject to an extensive set of exceptions relating to insurance functions. Neither Subtitle A nor the regulations of

[11]Under the 2000 Model Regulation, "licensee" means all licensed insurers, producers, and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the insurance law of the state.

the federal depository institution regulators or FTC separately address health information.[12]

A Majority of States Have Adopted the 2000 Model Regulation

As of March 1, 2002, 35 states and the District of Columbia have adopted statutes or regulations that are based on the 2000 Model Regulation.[13] Of those 36 jurisdictions, 2—Vermont and New Mexico—substituted an opt-in requirement, which can provide greater privacy protection, for the 2000 Model Regulation's opt-out provision.

Because New Mexico and Vermont substituted an opt-in requirement for the opt-out requirement, an insurance provider in these states generally is prohibited from disclosing nonpublic personal information to nonaffiliated third parties unless the provider first obtains the consumer's affirmative authorization to do so. Both states have retained the exception for disclosures to nonaffiliated third parties who perform functions or services for the institution and for joint marketing purposes. Vermont, however, limits the information that can be disclosed for joint marketing purposes to the consumer's name, contact information, and the institution's own transaction and experience information, because that information is defined under the Fair Credit Reporting Act (FCRA)[14] and Vermont's own fair credit reporting act.

[12]Pursuant to regulations promulgated by the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.), institutions covered by HIPAA that electronically maintain or transmit individually identifiable health information generally must obtain written authorization before disclosing such information. Some institutions subject to Subtitle A also may be subject to the HHS regulations. See the FTC Subtitle A regulations, Privacy of Consumer Health Information, 65 Fed. Reg. 33648. (May 24, 2000).

[13]For a complete listing of the 35 states, see appendix I.

[14]FCRA regulates the collection and dissemination of personal information by consumer reporting agencies.

Fourteen States That Continue to Rely on the 1982 Model Act Took Steps to Achieve Compliance with Subtitle A Requirements

As of March 1, 2002, 14 states were relying on previously enacted laws that are based on the 1982 Model Act but had amended their laws or taken administrative measures to ensure compliance with Subtitle A's provisions. A number of the 14 Model Act states told us that they did not adopt the 2000 Model Regulation because their existing laws and regulations, together with any additional requirements under Subtitle A, generally provided more protections for their residents. However, all of the 14 states took varying actions to ensure compliance with Subtitle A's annual notice requirement and requirements governing the content of the notices sent to customers. Although the 1982 Model Act contains additional protections not provided by Subtitle A, a number of the Model Act states modified some of the more protective provisions of their laws to obtain greater consistency with the less restrictive requirements of Subtitle A.

NAIC issued the Model Act in 1982 to address privacy concerns relating to the collection and disclosure of insurance information by insurance institutions, insurance agents, and organizations that assemble and provide information to insurers. Three of the 14 Model Act states—California, Connecticut, and Nevada—told us that they were in the process of adopting regulations, which would be based on the 2000 Model Regulation, to clarify or supplement their existing requirements. The remaining 11 states indicated that they planned to maintain their existing insurance laws with some modifications, because they believed that the privacy provisions contained in those laws meet or exceed Subtitle A requirements in most areas.

As an illustration from one of the Model Act states, the Montana State Auditor's Office, Insurance Department, stated that "… a decision was made to keep Montana's existing Privacy Act. It was already substantially compliant with GLBA and contained many important consumer protections that the current NAIC model privacy regulations do not provide for." In particular, the Insurance Department cited the requirement to provide notice of adverse underwriting decisions, the right to access recorded personal information, and the protection of all personal information as additional protections provided by Montana's law. Another example comes from the Ohio Department of Insurance, which explained, "Early in the process, the Ohio Department of Insurance considered adopting the recent NAIC Privacy Model [Regulation][sic]. However, the department concluded that current law already meets or exceeds the recent Model [Regulation's][sic] protections in most areas."

States Made Modifications to the 1982 Model Act to Ensure Compliance with Subtitle A

The Model Act states recognized that changes were needed in two areas to make their laws and regulations fully consistent with Subtitle A's requirements. First, although the 1982 Model Act requires insurance providers to give applicants and policyholders a notice of its information collection practices, the 1982 Model Act does not contain an annual notice requirement. Second, the content requirements for notices under the 1982 Model Act differ from the requirements in Subtitle A. While the notice required by the 1982 Model Act must describe the types of personal information that may be collected on an individual and the sources and investigative techniques that may be used to collect such information, the 1982 Model Act does not require that the privacy notice contain specific information on an institution's policies and practices for protecting privacy and information security.

Despite differing approaches to the notice requirements, all of the Model Act states have taken measures to ensure compliance with Subtitle A. Arizona, for example, amended its law to require annual notice to customers and to provide that a notice containing the information required by Subtitle A also satisfies the content requirements of the state's law if the notice also informs the individual of his or her right to access and correct information obtained by an insurance provider. Oregon issued regulations requiring that notices of insurance information practices must also contain information prescribed by Subtitle A. Other states have not amended their notice content requirements but still require their insurance providers to furnish their policyholders and applicants with notices containing the information specified in both the 1982 Model Act and Subtitle A.

Some Provisions of the 1982 Model Act May Provide Greater Protections than Subtitle A

The 1982 Model Act contains some protections not found in Subtitle A. For example, the 1982 Model Act contains a requirement that adverse underwriting decisions be adequately explained and establishes the right of an individual to access and correct personal information obtained by insurance providers. Other differences between the 1982 Model Act and Subtitle A may also result in greater protections being provided to insurance consumers.

As a general rule, the 1982 Model Act does not allow the disclosure of personal information without the affirmative consent of the individual; that is, the individual must opt in before protected information can be shared. In contrast, Subtitle A requires financial institutions to provide an opt-out opportunity before information can be shared. Opt-out provisions are generally perceived as being less restrictive or protective than opt-in

provisions, since under opt-out provisions, consumers must take action to stop the sharing of their information with nonaffiliated third parties. A number of state insurance officials we contacted referred to the opt-in requirement in the 1982 Model Act as a reason for not adopting the 2000 Model Regulation.

The 1982 Model Act permits the disclosure of personal information to nonaffiliates for the marketing of a product or service, but only if the individual is given the opportunity to opt out of the disclosure.[15] The 1982 Model Act also restricts the type of information that can be disclosed pursuant to this opt-out requirement. In comparison, Subtitle A specifically allows financial institutions to disclose nonpublic personal information to a nonaffiliated third party in connection with the marketing of financial products or services without allowing consumers an opportunity to opt out, subject to restrictions on subsequent disclosures by the recipient.

The 1982 Model Act also limits the disclosure of personal information to affiliates. Under the 1982 Model Act, disclosure to an affiliate whose only use of the information will be in connection with an audit of the insurance institution or the marketing of an insurance product or service is permitted only if the affiliate does not redisclose the information it obtains for another purpose or to unaffiliated persons.[16] Subtitle A does not restrict the sharing of nonpublic personal information among affiliates.

Some Model Act States Amended Their More Restrictive Marketing Disclosure Requirements

The Model Act states' approaches to the stricter restrictions on marketing disclosures and affiliate sharing of information are not uniform. As of March 1, 2002, 3 Model Act states—North Carolina, Oregon, and Virginia—have modified their requirements to permit information sharing for marketing purposes without an opt-out requirement, similar to the joint marketing exception in Subtitle A. Montana has an exception that may permit certain types of marketing agreements, but not all. The remaining 10 Model Act states have not modified their marketing restrictions. In

[15]Certain types of information, such as medical record information or personal information relating to an individual's character, personal habits, mode of living, or general reputation may not be disclosed under this exception.

[16]Under FCRA, affiliates may share personal information subject to an opt-out requirement. This provision preempts state laws concerning the exchange of information among affiliates until January 1, 2004. The preemption does not apply to Vermont. See 15 U.S.C. § 1681t(b)(2), (d) (2000).

addition, Arizona, Oregon, and Virginia have expanded the exception for disclosures to affiliates for marketing purposes.

Most States Have Not Established Standards for Safeguarding Insurance Customer Information

As of March 1, 2002, only one state—New York—has satisfied the Subtitle A mandate that state insurance authorities establish standards for safeguarding insurance customer records and information. An additional state—California—has proposed regulations containing such standards. The other states appear to have been waiting for NAIC to adopt the model regulation, "Standards for Safeguarding Customer Information" (NAIC Model Safeguarding Regulation). In early April, NAIC adopted the Model Safeguarding Regulation. In contrast, the federal regulators charged with implementing Subtitle A, with the exception of FTC, issued final standards much earlier. FTC has received comments on proposed standards and is developing final rules. NAIC staff explained that the state insurance authorities were slower in establishing the standards due to a number of factors, such as the need to develop a flexible regulation to cover a wide range in the types and sizes of organizations. Most state insurance authorities still need to implement the NAIC Model Safeguarding Regulation, either by legislative or regulatory action or both. During this period, insurance customers in these states might have reduced assurances that they will have a level of legal protection over the security and confidentiality of their information consistent with that of the customers of other financial institutions.

Subtitle A Directs Federal and State Regulators to Establish Safeguarding Standards

Under a separate provision of Subtitle A, federal regulators and state insurance authorities are to establish standards for the institutions under their jurisdiction relating to safeguards for customer information and records. Standards for safeguarding customer information and records must be set forth as guidance to the extent practicable by the federal depository institution regulators and the National Credit Union Administration; the remaining federal regulators must establish the standards by rule. The state insurance authorities also are to implement the standards by rule. In establishing standards relating to administrative, technical, and physical safeguards, the state insurance authorities must address (1) the security and confidentiality of customer records and information, (2) protection against any anticipated threats or hazards, and (3) protection against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

NAIC developed and adopted a model regulation from which the various state insurance authorities can draft their own safeguarding standards. The NAIC Model Safeguarding Regulation requires licensees to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of customer information. The NAIC Model Safeguarding Regulation also describes three objectives that a licensee's information security program shall be designed to accomplish, along with examples of the methods that a licensee should use in implementing an information security program. For example, the NAIC Model Safeguarding Regulation requires that a licensee (1) identify reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems and (2) assess the likelihood of and potential damage from these threats.

The NAIC Model Safeguarding Regulation generally is based on the guidelines of the federal depository institution regulators, but they differ from the federal guidelines in some respects. For example, the federal depository institution regulators have provided depository institutions with mandatory standards for the assessment of risk, the management and control of risk, and the oversight of service provider arrangements. The NAIC Model Safeguarding Regulation enumerates the same standards but characterizes them as examples of actions and procedures that a licensee may follow to achieve adequate information security of customer information and records. We were advised by NAIC staff that the NAIC Model Safeguarding Regulation was not as detailed as the federal depository institution regulators' guidelines because state insurance authorities oversee a much more diverse group of institutions.

State Insurance Authorities Are Taking More Time to Establish Safeguarding Standards than Most of the Federal Regulators

State insurance authorities have been slower to establish safeguarding standards than most of the federal regulators. NAIC completed its initial draft of the model standards in late spring 2001. In comparison, all but one of the federal regulators charged with implementing Subtitle A have adopted safeguarding standards. The federal depository institution regulators issued their standards on safeguarding customer records and information on February 1, 2001.[17] The Securities and Exchange Commission and Commodities Futures Trading Commission issued their

[17]The National Credit Union Administration issued its guidelines for safeguarding customer records and information on January 30, 2001.

rules to safeguard customer record information last year, but they essentially restated the language used in Subtitle A. As of March 1, 2002, FTC has not issued final standards on safeguarding customer records and information but expects to issue its final rule in a couple of months. According to an FTC attorney, extra time was needed to develop appropriate standards because the range of financial institutions that FTC oversees under Subtitle A is so broad. Specifically, FTC has jurisdiction over all financial institutions that are not subject to the jurisdiction of another agency or authority under Subtitle A, including such diverse entities as nondepository lenders, individual tax preparers, automobile dealers, and mortgage brokers. For many of the smaller organizations that are covered, procedures for securing customer records and information may be new. Therefore, it took FTC staff time to develop the appropriate safeguarding standards.

According to NAIC, a number of factors affected the process it followed in drafting and adopting the Model Safeguarding Regulation.

- NAIC waited for the federal agencies to take action on the matter so that they could use the federal guidelines as a template. NAIC's goal was to be as uniform as possible so insurers would not be at a competitive disadvantage in comparison to other financial services providers. Unlike the 2000 Model Privacy Regulation, NAIC was not able to follow the federal guidelines in developing the model standards because it felt that the guidelines would not have worked effectively for insurers. Specifically, NAIC felt that the guidelines issued by the federal depository institution regulators were too detailed and specific to depository institutions, and that the standards contained in the Securities and Exchange Commission's regulations were too general.

- NAIC stated that it developed its model standards through a very open deliberative process that allowed them to be thoroughly reviewed and debated by all interested parties. The first draft of the NAIC Model Safeguarding Regulation was issued in June 2001. The initial public hearing on the model was scheduled to take place at the NAIC Fall National Meeting in September; however, that meeting was cancelled due to the September 11 terrorist attacks. The hearing was subsequently held at the NAIC Winter National Meeting in December 2001. The draft standards went through two public written comment periods and oral comments were taken again at the NAIC Spring National Meeting in March 2002.

- NAIC noted that the state regulatory structure for the insurance industry affects the time it will take for the states to implement Subtitle A's safeguarding provisions. Each state has its own procedures that must be followed when a regulation is developed, and most—if not all—state insurance authorities have no authority to promulgate regulation based on a federal law. State insurance authorities obtained their authority from their state laws.

- NAIC staff told us that the model standards were designed to establish a flexible standard that all insurance entities can meet. They believe this flexibility is important because state insurance departments regulate many different types and sizes of organizations, all of which will be required to comply with this rule. NAIC staff pointed out the challenge of developing a regulation to cover a wide range of types and sizes of organizations was similar to that faced by FTC.

New York and California Are Ahead of the Other States in Establishing Safeguarding Standards

New York has carried out the Subtitle A mandate to establish standards for safeguarding insurance customer records and information. The New York Department of Insurance adopted Regulation 173, "Standards for Safeguarding Customer Information," on February 27, 2002. California issued a proposed regulation that contains safeguarding standards for public comment on December 4, 2001. Both New York's Regulation 173 and California's proposed regulations are generally consistent with the current draft of NAIC Model Safeguarding Regulation. Currently, the California Insurance Department is reviewing the public comments it has received. A California Insurance Department official could not provide us with the exact date that a final regulation would likely be issued.

The Remaining States Will Likely Need Some Time before Adopting Safeguarding Standards

Although NAIC has developed model standards, it is likely that it will take months for many of the remaining 48 states to adopt safeguarding standards. As an illustration, according to an NAIC document, 8 states still had regulations pending to implement Subtitle A's notice and disclosure requirements almost a year after NAIC had finalized its 2000 Model Regulation. An NAIC official told us that after the 2000 Model Regulation went to the states, some state insurance commissioners could not promulgate the required regulations until their respective state legislatures provided them with the statutory authority to issue regulations. Moreover, some state insurance authorities may be required to comply with a specific administrative procedure, such as providing a public comment period before a final regulation can be issued. During the time it takes for the states to issue safeguarding standards, insurance customers in these states

might have reduced assurances that they will have a level of legal protection over the security and confidentiality of their information consistent with that of the customers of banking and securities companies.

Conclusions

All 50 states and the District of Columbia have generally followed one of two approaches to ensuring insurance industry compliance with the disclosure requirements of Subtitle A. Most of the states have adopted regulations or legislation based on the 2000 Model Regulation, which generally is comparable with the regulations issued by the federal depository institution regulators and FTC. However, a number of states have decided to retain their versions of the 1982 Model Act—which several states view as providing greater privacy protections than Subtitle A—with some modifications to ensure compliance with all of Subtitle A's requirements. In addition, some states have modified or retained certain provisions of their laws and regulations to provide insurance consumers with greater protections than required by Subtitle A. Such actions are consistent with Subtitle A, as Congress specifically allowed states to enact statutes or issue regulations, orders, and interpretations that provide greater financial privacy protections than is contained in Subtitle A.

State insurance authorities are behind most of the federal regulators in establishing standards for safeguarding the nonpublic personal information of consumers as required by Subtitle A. NAIC's adoption of a model for states to use in developing the required standards is an important first step. Although NAIC has approved the model standards, there is no guarantee that all states will consistently implement the NAIC Model Safeguarding Regulation. Each state must independently take action to implement the NAIC Model Safeguarding Regulation. During this period, the security and the confidentiality of insurance customer information and records may not be subject to a consistent level of legal protections envisioned by Subtitle A.

Agency Comments and Our Evaluation

We requested comments on a draft of this report from NAIC. On March 28, 2002, NAIC's Senior Counsel for Financial Services provided us with the following oral comments on the draft. Although NAIC felt that the statements made in the draft report were generally technically accurate, it was concerned about what it perceived as an overall negative tone of the draft. NAIC wanted the report to reflect that since enactment of GLBA, the states have worked hard and accomplished a great deal to meet the congressionally mandated requirements of the law. According to NAIC, this activity has taken place with respect to a very controversial and

politically charged issue, and, unlike the federal agencies with direct authority from Congress, the state regulators had to look for authority from their individual state legislatures. NAIC emphasized that, nonetheless, to date, every state except Alaska has privacy protections in place that meet or exceed the standards established in GLBA.

In addition, NAIC was concerned about some of the specific wording used in the draft regarding the progress states were making in promulgating regulations requiring insurance licensees to meet the confidentiality and security requirements set forth in Subtitle A's safeguarding provisions. NAIC staff said that the states have been responsive on this issue and have continued to work to satisfy the congressional mandate. NAIC also provided greater details on the factors that affected the process it followed in drafting and adopting the Model Safeguarding Regulation. In response to NAIC's comments, we expanded our discussion in this report on the factors affecting the adoption of the Model Safeguarding Regulation and included the additional details provided by NAIC. In addition, NAIC staff provided technical comments, which we have incorporated where appropriate. We also obtained technical comments from FTC staff, which we also incorporated where appropriate.

Scope and Methodology

To understand the legislative requirements for states relating to the protection of insurance information of consumers, we reviewed Subtitle A, Title V of GLBA. To determine the specific legislative and regulatory actions taken by the states to carry out the provisions of Subtitle A relating to the insurance industry, we used publicly available data from NAIC. We did not attempt to independently verify NAIC data. In addition, we reviewed the 2000 Model Regulation and the 1982 Model Act. To obtain information on insurance privacy laws that are based on the 1982 Model Act, we sent a list of questions to the 14 state insurance authorities that continue to rely on such laws, and we requested written responses to the questions. All 14 state insurance authorities provided us with written responses to our questions.

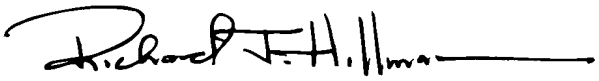
To ascertain the progress states have made to implement the Subtitle A mandate that they establish standards for safeguarding insurance customer records and information, we reviewed NAIC's model standards for safeguarding customer information and New York and California's draft regulations relating to the standards for safeguarding customer information. In addition, we interviewed two representatives of the NAIC Privacy Working Group, which developed the model standards.

We performed our work between July 2001 and March 2002 in Washington, D.C., in accordance with generally accepted government auditing standards.

As agreed with your office, unless you publicly release its contents earlier, we plan no further distribution of this report until 30 days from its date. At that time, we will send copies of this report to the chairman of the House Committee on Energy and Commerce as well as to the chairmen and ranking minority members of the Senate Committee on Banking, Housing, and Urban Affairs and the House Committee on Financial Services. We will also send copies of this report to the president of NAIC and to the chairman of the Federal Trade Commission and make copies available to other interested parties upon request.

If you or your staff have any questions on this report, please contact me at (202) 512-8678 or Harry Medina at (415) 904-2000. Key contributors to this report were Nancy Eibeck, Janet Fong, Barbara Roesmann, and Paul Thompson.

Sincerely yours,



Richard J. Hillman
Director, Financial Markets and
Community Investment

Appendix I: State Actions to Implement Title V, Subtitle A of the Gramm-Leach-Bliley Act

State	2000 Model Regulation	1982 Model Act
Alabama	X	
Alaska[a]		
Arizona		X
Arkansas	X	
California		X
Colorado	X	
Connecticut		X
Delaware	X	
District of Columbia	X	
Florida	X	
Georgia		X
Hawaii	X	
Idaho	X	
Illinois	X	
Indiana	X	
Iowa	X	
Kansas	X	
Kentucky	X	
Louisiana	X	
Maine		X
Maryland	X	
Massachusetts		X
Michigan	X	
Minnesota		X
Mississippi	X	
Missouri	X	
Montana		X
Nebraska	X	
Nevada		X
New Hampshire	X	
New Jersey		X
New Mexico	X	
New York	X	
North Carolina		X
North Dakota	X	
Ohio		X
Oklahoma	X	
Oregon		X
Pennsylvania	X	
Rhode Island	X	
South Carolina	X	
South Dakota	X	

State	2000 Model Regulation	1982 Model Act
Tennessee	X	
Texas	X	
Utah	X	
Vermont	X	
Virginia		X
Washington	X	
West Virginia	X	
Wisconsin	X	
Wyoming	X	

[a]As of March 1, 2002, privacy regulations are pending.

Source: National Association of Insurance Commissioners.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548